EXHIBIT A

IN THE COURT OF COMMON PLEAS OF FRANKLIN COUNTY, PENNSYLVANIA
CIVIL DIVISION

K.H., a minor, and S.H., a minor, by VIRGINIA JOHNSON, Guardian, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	No. 2022-3277
v.	)	
KEYSTONE RURAL HEALTH CENTER, d/b/a KEYSTONE HEALTH,	)	Judge
Defendant.	)	JURY TRIAL DEMANDED

JUDGE: Jeremiah D. Zook

CLASS ACTION COMPLAINT

Plaintiffs K.H., a minor, and S.H., a minor, by Virginia Johnson, Guardian ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through the undersigned attorneys, brings this Class Action Complaint against Defendant Keystone Rural Health Center (d/b/a Keystone Health) ("Keystone") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Keystone for its failure to secure and safeguard Plaintiffs' and approximately 235,237 other individuals' personal health information ("PHI") and personally identifiable information ("PII"), including "names, Social Security numbers, and clinical information."[1]

[1] *Notice of Security Incident*, KEYSTONE HEALTH, https://keystonehealth.org/wp-content/notice_pdf/notice_of_security_incident.pdf (last accessed Oct 21, 2022).

2. Defendant is a healthcare provider with its principal place of business in Chambersburg, Pennsylvania. It provides medical care and other services to persons throughout Pennsylvania.

3. Between July 28, 2022 and August 19, 2022, unauthorized individuals gained access to Keystone's networks and accessed the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. Keystone promised Plaintiffs and Class members that it would implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Keystone breached those promises by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect its patients' and former patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Keystone's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all United States residents whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiffs, on behalf of themselves and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiffs K.H., a minor, and S.H., a minor, and their parent and guardian Virginia Johnson, are Pennsylvania residents. K.H. and S.H. received services from Keystone. Believing Keystone would implement and maintain reasonable security and practices to protect their PII/PHI, Plaintiffs provided their PII/PHI to Keystone in connection with receiving services. Plaintiffs received letters from Keystone notifying them that their PII/PHI may have been exposed in the Data Breach. Had Plaintiffs known that Keystone does not adequately protect PII/PHI, they would not have agreed to provide Keystone with their PII/PHI or used Keystone's services.

8. Defendant Keystone Rural Health Center, d/b/a Keystone Health, is a Pennsylvania corporation with a principal place of business located at 111 Chambers Hill Drive, Suite 200, Chambersburg, Pennsylvania 17201.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this matter pursuant to 42 Pa. C.S. § 931. Further, Plaintiffs and the Class seek damages in excess of $50,000.

10. This Court has personal jurisdiction over Keystone pursuant to 42 Pa. C.S. § 5301 because Keystone is a corporation formed under the laws of Pennsylvania, and it carries on a continuous and systemic part of its business within Pennsylvania.

11. Venue is proper in Franklin County because Keystone's principal place of business is located in Franklin County and Keystone regularly conducts business in Franklin County.

FACTUAL ALLEGATIONS

Overview of Keystone

12. Keystone's principal place of business is located in Chambersburg, Pennsylvania.[2]

[2] *See Homepage*, KEYSTONE, https://keystonehealth.org/ (last visited Oct. 21, 2022).

Per its website, Keystone physicians and staff provide a comprehensive range of medical services, including primary care, dental care, pediatrics, and pharmacy services.[3]

13. In the regular course of its business, Keystone collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health- or medical-related services.

14. Keystone requires patients to provide personal information before it provides treatment at its facilities. That information includes, *inter alia*, names, dates of birth, addresses, insurance information, and Social Security numbers. Keystone also creates, collects, and stores other PII/PHI of its patients and former patients, including diagnosis and treatment information, and date(s) of service. Keystone stores this information digitally.

15. Keystone's website contains a "Notice of Privacy Practices," available in the "Patient Information" section of its website. The Notice of Privacy Practices states "[Keystone] will not use or share your information other than as described [in the Notice] unless you tell us we can in writing."[4] In the same Notice of Privacy Practices, Keystone acknowledges it is "required by law to maintain the privacy and security of your protected health information."[5]

16. Despite this acknowledgment and the assertions and promises in its Notice of Privacy Practices to safeguard PII/PHI, Keystone fails and has failed to adequately protect patients' PII/PHI.

17. Plaintiffs and Class members are, or were, patients or former patients of Keystone or received health-related services from Keystone, and entrusted Keystone with their PII/PHI.

---

[3] *See About Us*, KEYSTONE, https://keystonehealth.org/about-us/ (last visited Oct. 21, 2022).
[4] *Notice of Privacy Practices*, KEYSTONE, https://keystonehealth.org/wp-content/uploads/2019/01/notice-of-privacy-practices-January-2019.pdf (last visited Oct. 21, 2022).
[5] *Id.*

The Data Breach

18. Between July 28, 2022 and August 19, 2022, an unauthorized individual, or unauthorized individuals, gained access to Keystone's computer systems.[6] Analysis of the Data Breach indicates that files containing patient PII/PHI were accessed by unauthorized individuals.[7]

19. According to the U.S. Department of Health and Human Services, 235,237 individuals' PII/PHI was exposed during the breach.[8]

20. Keystone did not begin to notify impacted breach victims about the data breach until October of 2022. The notice Keystone posted on its website states the information that was accessed included "names, Social Security numbers, and clinical information."[9]

Keystone Knew that Criminals Target PII/PHI

21. At all relevant times, Keystone knew, or should have known, its patients', Plaintiffs', and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, Keystone failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that Keystone should have anticipated and guarded against.

22. It is well known amongst companies that store sensitive personally identifying information that sensitive information—like the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses,

---

[6] *Notice of Security Incident*, *supra* note 1.
[7] *Id.*
[8] *Cases Currently Under Investigation*, DEP'T HEALTH AND HUMAN SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Oct. 21, 2022).
[9] *Notice of Security Incident*, *supra* note 1.

including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[10]

23. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus, found that there were 905 medical data breaches in 2021 with over 50 million patient records exposed.[11] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[12]

24. PII/PHI is a valuable property right.[13] The value of PII/PHI as a commodity is measurable.[14] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[15] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[16] PII/PHI is so valuable to identity thieves that once it has been disclosed, criminals often trade it on the black market for many years.

---

[10] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[11] PROTENUS, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last visited Oct. 21, 2022).

[12] *Id.*

[13] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible..."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[14] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[15] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[16] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

25. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

26. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[17] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[18] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[19]

27. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[20] According to a report released by the Federal Bureau of Investigation's

---

[17] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[18] *Id.*

[19] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[20] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[21]

28. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[22] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[23]

29. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[24]

Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

30. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and

---

[21] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited Oct. 21, 2022).

[22] *What Happens to Stolen Healthcare Data*, *supra* note 17.

[23] *Id.*

[24] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

incur charges and credit in a person's name.[25]

31. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[26] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[27]

32. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[28]

---

[25] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Oct. 21, 2022).

[26] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

[27] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited Oct. 21, 2022).

[28] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Oct. 21, 2022).

33. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[29]

34. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

35. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[30]

36. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[31] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[32] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get

---

[29] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Oct. 21, 2022).

[30] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[31] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[32] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk…*, *supra* note 21.

prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [33] The FTC also warns, ""If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[34]

37. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[35]

---

[33] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Oct. 21, 2022).
[34] *Id.*
[35] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 31.

38. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[36]

39. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

40. Plaintiffs and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

41. This action is brought and may be properly maintained as a class action pursuant to Pa.R.Civ.P. 1702.

---

[36] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

42. Plaintiffs brings this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All United States residents whose PII/PHI was accessed in the Data Breach by unauthorized persons, including all United States residents who were sent a notice of the Data Breach.

43. Excluded from the Class is Keystone Rural Health Center, d/b/a Keystone Health, and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

44. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

45. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. The U.S. Department of Health and Human Services reports that 235,237 individuals' information was exposed in the Data Breach.

46. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether an implied contract existed between Class members and Keystone providing that Keystone would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Keystone was unjustly enriched due to its promises to safeguard Class members' PII/PHI and its failure to do so;

c. Whether Keystone engaged in unfair or deceptive acts in violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law; and

d. Whether Plaintiffs and all other Class members are entitled to damages, and the measure of such damages and relief.

47. Keystone engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

48. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Keystone, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

49. Plaintiffs will fairly and adequately represent the interests of the Class members. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature. Plaintiffs have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs and their counsel have adequate resources to assure the interests of the Class will be adequately represented.

50. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Keystone, so it would be impracticable for

Class members to individually seek redress from Keystone's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

51. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

52. Keystone owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

53. Keystone knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure systems. Keystone knew of the many data breaches that targeted health care providers in recent years.

54. Given the nature of Keystone's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Keystone should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

55. Keystone breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware

systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class members' PII/PHI.

56. It was, or should have been, reasonably foreseeable to Keystone that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

57. But for Keystone's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised.

58. As a result of Keystone's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security..

COUNT II
NEGLIGENCE PER SE

59. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

60. Keystone's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

61. Keystone's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Keystone, of failing to employ reasonable measures to protect and secure PII/PHI.

62. Keystone violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and not complying with applicable industry standards. Keystone's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

63. Keystone's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

64. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

65. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

66. It was reasonably foreseeable to Keystone that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate

data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

67. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Keystone's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

68. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

69. Plaintiffs and Class members gave Keystone their PII/PHI in confidence, believing that Keystone would protect that information. Plaintiffs and Class members would not have provided Keystone with this information had they known it would not be adequately protected. Keystone's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between Keystone and Plaintiffs and Class members. In light

of this relationship, Keystone must act primarily for the benefit of its patients and former patients, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

70. Keystone has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

71. As a direct and proximate result of Keystone's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Keystone's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

72. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

73. In connection with receiving medical services, Plaintiffs and all other Class members entered into implied contracts with Keystone.

74. Pursuant to these implied contracts, Plaintiffs and Class members paid money to Keystone, whether directly or through their insurers, and provided Keystone with their PII/PHI. In exchange, Keystone agreed to, among other things, and Plaintiffs understood that Keystone would: (1) provide medical services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; and (3) protect Plaintiffs' and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

75. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Keystone, on the other hand. Indeed, as set forth *supra*, Keystone recognized its duty to provide adequate data security and ensure the privacy of its patients' PII/PHI in its Notice of Privacy Practices. Had Plaintiffs and Class members known that Keystone would not adequately protect its patients' and former patients' PII/PHI, they would not have received services from Keystone.

76. Plaintiffs and Class members performed their obligations under the implied contract when they provided Keystone with their PII/PHI and paid—directly or through their insurers—for health care or other services from Keystone.

77. Keystone breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

78. Keystone's breach of its obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

79. Plaintiffs and all other Class members were damaged by Keystone's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk or imminent threat of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

80. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

81. This claim is pleaded in the alternative to the breach of implied contract claim.

82. Plaintiffs and Class members conferred a monetary benefit upon Keystone in the form of monies paid for health care services or other services.

83. Keystone accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Keystone also benefitted from the receipt of Plaintiffs' and Class members' PHI, as this was used to facilitate payment.

84. As a result of Keystone's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class

members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

85. Keystone should not be permitted to retain the money belonging to Plaintiffs and Class members because Keystone failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

86. Keystone should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("UTPCPL")
73 P.S. §§ 201-1–201-9.3

87. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

88. Keystone performs services in the Commonwealth of Pennsylvania.

89. Plaintiffs, Class members, and Keystone are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

90. Keystone's health care and other services constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

91. Keystone obtained Plaintiffs' and Class members' PII/PHI in connection with the health care and other services that Keystone performed.

92. Keystone engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to protect and secure their

patients' and former patients' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards.

93. Keystone makes explicit statements to their customers that their PII/PHI will remain private, as evidenced by its Notice of Privacy Policy.

94. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). Keystone's failure to adequately protect Plaintiffs and Class members' PII/PHI while holding out that it would adequately protect the PII/PHI falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

95. Due to the Data Breach, Plaintiffs and Class members have lost property in the form of their PII/PHI. Further, Keystone's failure to adopt reasonable practices in protecting and safeguarding their customers' PII/PHI will force Plaintiffs and Class members to spend time or money to protect against identity theft. Plaintiffs and Class members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Keystone's practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

96. As a result of Keystone's violations of the UTPCPL, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased or imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

97. Pursuant to 73 P.S. § 201-9.2(a), Plaintiffs seek actual damages, $100, or three times their actual damages, whichever is greatest. Plaintiffs also seek costs and reasonable attorney fees.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Keystone as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representative, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Keystone from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide

or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: October 21, 2022

Respectfully submitted,

/s/ Mark B. DeSanto

Mark B. DeSanto (320310)
Joseph B. Kenney (316557)
SAUDER SCHELKOPF, LLC
1109 Lancaster Avenue
Berwyn, PA 19312
Tel: 888.711.9975
Fax: 610.727.4360
mbd@sstriallawyers.com
jbk@sstriallawyers.com

Ben Barnow*
Anthony L. Parkhill*
Riley W. Prince*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com

**Pro hac vice* to be submitted